



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

General Position Information

Job Title: PE634 - Chief, Security Architecture & Engineering Group - GS-15

Salary Range: \$108,887 - \$160,300

Vacancy Open Period: 12/13/2016 – 01/03/2017

Position Type: Cadre

Who May Apply: External Candidates (Staff Reserve Only), Internal ODNI Candidates, Detailees

Division: CIO/CIO

Duty Location: Bethesda, MD

Security Clearance: TS/SCI with CI Polygraph

Travel Required: 0-25% Travel

Relocation Expenses: Not Authorized

Job Interview Travel: Candidates from outside the Washington, D.C., area may be selected for a telephone, teleconference, or in-person interview. If selected for an in-person interview, any travel or lodging will be at the applicant's personal expense.

Position Information

This is an opportunity for:

- An internal or external candidate to fill a GS-15 cadre (Staff Reserve) position. Staff Reserve appointments are time-limited appointments made for a period of up to 3 years, with a possible extension up to 2 additional years.

Who May Apply

Current GS employees at the same grade or one grade lower than the advertised position grade may apply.

Former members of the Peace Corps may be considered for ODNI employment only if five full years have elapsed since separation from the Peace Corps.

- For a cadre assignment:
 - Current ODNI cadre.
 - Current ODNI Staff Reserve Employees. (A staff reserve employee who currently occupies this position may not apply.)
 - Current Federal Government employees.
 - Candidates outside the Federal Government.



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

**** Staff Reserve appointments are time-limited appointments made for a period of up to 3 years, with a possible extension up to 2 additional years.****

Salary Determination

- The ODNI uses a rank-in-person system in which rank is attached to the individual. A selected ODNI candidate or other Federal Government candidate will be assigned to the position at the employee's current GS grade and salary.
- For a selected non-Federal Government candidate, salary will be established within the salary range listed above, based on education and experience.

Component Mission

The IC CIO's mission is to improve the collective effectiveness and information sharing of intelligence organizations' support the intelligence mission. The IC CIO reports directly to the Director of National Intelligence and has four primary strategic initiatives that directly support the Director's National Intelligence Strategy (NIS). The four Strategic Initiatives are: • Enhance Cyber Security (NIS Mission Objective 5) • Support Current Operations [e.g., Middle East, Counterterrorism, etc.] (NIS Mission Objective 6) • IC Business Transformation (NIS Enterprise Objective 3) • Improve Information Integration and Information Sharing (NIS Enterprise Objective 4)

Major Duties and Responsibilities (MDRs)

- Chief, Security Architecture & Engineering Group, IAD Division on all on security and technical related matters, formulating integrated policies for information assurance principles to guide secure technology decisions. - Enable Intelligence Community (IC) mission through the development of system security concepts and capabilities that improve the safeguarding IC data and systems. - Lead and manage complex computer engineering projects or programs that may have ill-defined requirements, ambiguity, parallel tasks, multiple dependencies, high risks, and multiple interfaces; manage the design, construction, testing, and implementation of technical and functional specifications; provide technical oversight and initiate, plan, implement, and coordinate activities throughout the life of the project. - Lead the drafting and coordination of all IC CIO technical specifications, and policies, in accordance with IC's Enterprise Architecture to ensure security practices are streamlined and then integrated into transformed business practices. - Conduct technical research and apply best practices and processes for capturing, refining, and assisting in prioritization of security requirements based on risk, system security engineering principles, and mission requirements. - Provide cybersecurity requirements and facilitate the translation of these requirements into secure technical solutions that can be understood by adopters, implementers, and developers. - Provide guidance to customers about applicability of information systems security solutions to meet mission needs. - Oversee the effective integration and interoperability of disparate cybersecurity related capabilities developed by separate service providers. - Consult with customers to gather and evaluate security architectures, designs, and system configuration information that facilitate secure missions systems.

Mandatory and Educational Requirements

- Expert experience in cross community complex programs and making expert recommendations to improve products and services; considerable ability to deal with service failures and prioritize customer needs. - Superior



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

ability to manage an Information Assurance/ Cybersecurity program, project, or process employing related skills such as objective and requirements development, task break out, developing schedules and budgets, identifying risks and opportunities, and identifying required resources. - Superior interpersonal, organizational, and problem-solving skills, including a demonstrated ability to work effectively both independently and in a team or collaborative environment and to lead and mentor junior colleagues. - Expert ability to communicate, both verbally and in writing, complex information in a clear, concise manner that is targeted to and meets the needs of diverse audiences with different perspectives and objectives. - Superior ability to listen to, clarify, and convey understanding of others' ideas, comments, and questions as well as to integrate and build upon diverse opinions in a manner that encourages the formation of integrated solutions and positions. - Expert ability to use knowledge and experience to look at a situation objectively, setting aside any biases, and determining the best long-term solution - Superior ability to develop and/or applying Information Assurance/ Cybersecurity principles, policies, practices, standards, and controls relevant to confidentiality, integrity, availability, authentication, and non-repudiation. - Superior ability to perform thorough work and conscientious about attending to detail. - Expert knowledge of network security architecture and systems security engineering concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth). - Expert knowledge of design, development, and interconnectivity in problem analysis, structured analysis and design, and or programming techniques. - Expert ability to quickly identify and apply new technologies, methodologies, and technical languages. - Expert ability to capture and refine information security requirements and ensure the requirements are integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration.

Desired Requirements

- Experience -One year of specialized experience at the next lower GS-grade (or equivalent). IT related experience may be demonstrated by paid or unpaid experience and/or completion of specific, intensive training (for example, IT Certification). IT- related experience demonstrating each of the four competencies (Attention to Detail, Customer Service, Oral Communication, and Problem Solving). Degree in computer science, engineering, information science, information systems management, mathematics, operations research, statistics, or technology management or degree that provided a minimum 24 semester hours in one or more of the fields identified above and required the development or adaptation of applications, systems or networks.

Key Requirements and How To Apply

Internal ODNI Candidates:

A complete application package must include:

- a. **RESUME:** Applicants are encouraged to carefully review the vacancy announcement, particularly the MDRs, and construct their resume to highlight their most significant experience and qualifications relevant to this job opportunity.
- b. **PERFORMANCE EVALUATIONS:** Applicants are required to provide their two most recent performance evaluations. A justification is required if the applicant is unable to provide the two most recent evaluations.
- c. **VACANCY NUMBER:** Reference the vacancy number in the subject line of the email and on each document submitted.



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

- d. **COVER LETTER:** Applicants must submit a cover letter as a supplement to the resume to elaborate on their qualifications and previous work performed.

WHERE TO SUBMIT: Applications should be sent to either DNI-MSD-HR-RR-Team_A_WMA@dni.ic.gov (classified email system) or Recruitment_TeamA@dni.gov (unclassified email system). Applicants submitting via JWICS are requested to submit their materials to both saksdav@dni.ic.gov (*David S.*) and mcreaz@cia.ic.gov (*Zina M.*) in lieu of the group address above. All attachments should be in Microsoft Word or Adobe PDF format.

Applications submitted through the classified email system should NOT contain classified information above the TS//SI/TK//NOFORN level.

Current Federal Employees Applying for a Detail Assignment:

Applicants from federal agencies within the Intelligence Community (IC) may be considered for this position as a reimbursable detailee, if endorsed by the employing agency. Must have current TS/SCI with polygraph or have the ability to obtain one. DNI does not provide polygraphs or security clearance for detailees. Applicants from within the IC must submit an application through the classified IC Joint Duty Program website.

Applicants from federal agencies outside the IC must provide written endorsement, concurring on the detail, from their employing agency. If approved to apply for the ODNI detail assignment, they must include the following in their application package:

- a. **RESUME** - All applicants must submit a resume addressing the MDRs, Mandatory and Desired Position Requirements. Format is at the discretion of the applicant, but must include full name, address, telephone number and email address.
- b. **PERFORMANCE EVALUATIONS** - Applicants are required to provide their two most recent performance evaluations as part of the application package. A justification is required as part of the application package if the applicant is unable to provide the two most recent evaluations.
- c. **ENDORSEMENT:** Employing element nomination/endorsement concurring on the detail.
- d. **VACANCY NUMBER** - Reference the vacancy number in the subject line of the email and on each document submitted.
- e. **CLEARANCE:** Must have a current TS/SCI with polygraph or have the ability to obtain one. DNI does not provide polygraphs or security clearances for detailees.

WHERE TO SUBMIT: Applications should be sent to either DNI-MSD-HR-RR-Team_A_WMA@dni.ic.gov (classified email system) or Recruitment_TeamA@dni.gov (unclassified email system). Applicants submitting via JWICS are requested to submit their materials to both saksdav@dni.ic.gov (*David A. Saks*) and mcreaz@cia.ic.gov (*Zina M. McCreary*) in lieu of the group address above. All attachments should be in Microsoft Word or Adobe PDF format.

Applications submitted through the classified email system should NOT contain classified information above the TS//SI/TK//NOFORN level.



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

External Candidates:

Key Requirements:

- U.S. Citizenship.
- Successful completion of CI polygraph and background investigation.
- Successful completion of a ODNI medical screening.
- A two-year trial period is required for all new permanent appointments to the ODNI.

A complete application must include:

- a. **RESUME:** Applicants are encouraged to carefully review the vacancy announcement, particularly the MDRs, and construct their resume to highlight their most significant experience and qualifications relevant to this job opportunity.
- b. **VACANCY NUMBER:** Reference the vacancy number in the subject line of the email and on each document submitted.
- c. **COVER LETTER:** Applicants must submit a cover letter as a supplement to the resume to elaborate on their qualifications and previous work performed.
- d. **SF-50:** Current or former Federal Government employees must provide an SF-50, "Notification of Personnel Action" to verify current federal status, position, title, grade, and organization of record.

WHERE TO SUBMIT: Applications should be sent to Recruitment_TeamA@dni.gov (unclassified email system).

Applicants submitting via JWICS are requested to submit their materials to both saksdav@dni.ic.gov (*David S.*) and mccreaz@cia.ic.gov (*Zina M.*) in lieu of the group address above. All attachments should be in Microsoft Word or Adobe PDF format.

Applications submitted through the classified email system should NOT contain classified information above the TS//SI//TK//NOFORN level.

All Applicants:

APPLICATION PACKAGES MUST CONTAIN ALL ITEMS LISTED ABOVE. AN INCOMPLETE APPLICATION PACKAGE WILL BE INELIGIBLE FOR CONSIDERATION.

Your application MUST be received by midnight on the closing date of this announcement. Applications received after the closing date will NOT be eligible for consideration.

To verify receipt of your application package ONLY, you may call 703-275-3799.



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

What To Expect Next

The most highly qualified candidates will be referred to the hiring manager for further consideration and possible interview. We expect to make a selection within 30 days of the closing date of this announcement. Due to the large number of applications received, applicants will be contacted **ONLY** if they have been selected for an interview.

Agency Contact Information

ODNI Recruitment; Phone: 703-275-3799; Email: Recruitment_TeamA@dni.gov

Other Information

The ODNI offers a broad array of benefits programs and family friendly flexibilities for ODNI cadre.

- Federal Employees Health Benefits Program: <http://www.opm.gov/insure/health/index.asp>
- Life Insurance: <http://www.opm.gov/insure/life/index.asp>
- Long-Term Care Insurance: <http://www.ltcfeds.com>
- Federal Employees Retirement SYSTEM (FERS) (new employees automatically covered):
<http://www.opm.gov/retire/index.asp> If you are transferring from another agency and covered by the Civil Service Retirement System (CSRS), you may continue in that system.
- Annual and Sick Leave: <http://www.opm.gov/oca/leave/index.asp>
- Flexible Spending Accounts for Health Care and Dependent Care: <http://www.fsafeds.com/fsafeds/index.asp>
- Paid Federal Holidays
- Alternative Work Schedules

The ODNI is an equal opportunity employer and abides by applicable employment laws and regulations.

REASONABLE ACCOMMODATIONS FOR PERSONS WITH DISABILITIES: The ODNI provides reasonable accommodations to otherwise qualified applicants with disabilities. IF YOU NEED A REASONABLE ACCOMMODATION for any part of the application and hiring process, please notify the Intelligence Community Equal Employment Opportunity and Diversity Office Representative by classified email at DNI-EEOD-RA-ACF@exchange.cia.ic.gov, by unclassified email at DNI-EEOD@dni.gov, by telephone at 703-874-8360, by TTY at 703-874-8554, or by FAX at 703-874-8651. Your request for reasonable accommodation will be addressed on a case-by-case basis. **PLEASE DO NOT SUBMIT YOUR APPLICATION TO THE EEOD EMAIL ADDRESS. THIS EMAIL IS FOR REASONABLE ACCOMMODATION REQUESTS ONLY. PLEASE SUBMIT YOUR APPLICATION VIA THE EMAIL ADDRESS PROVIDED IN THE 'HOW TO APPLY' SECTION ABOVE.**